UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,252	01/31/2002	Massimiliano Antonio Poletto	12221-012001	2792

87555 7590 05/12/2009

Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
05/12/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MASSIMILIANO ANTIONIO POLETTO
and ANNE ELIZABETH DUDFIELD

Appeal 2009-0940
Application 10/066,252
Technology Center 2400

Decided:[1] May 12, 2009

Before LEE E. BARRETT, JOSEPH L. DIXON, and LANCE LEONARD BARRY, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] The two month time period for filing an appeal or commencing a civil action, as recited in 37 CFR § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date.

STATEMENT OF THE CASE

The Patent Examiner rejected claims 1-16, 24, 25, and 27-34. The Appellants appeal therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

INVENTION

The invention at issue is a monitoring device for thwarting denial of service ("DoS") attacks on a data center. More specifically, the device collects statistics on packets sent between a network and the data center. (Spec. 1.)

ILLUSTRATIVE CLAIM

1. A monitoring device disposed for thwarting denial of service attacks on a data center, the monitoring device comprising:

a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links and collect statistical information on packets that are sent between the network and the data center over the coupled physical links for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

PRIOR ART

Kim	US 2002/0069356 A1	Jun. 06, 2002 (Feb. 14, 2001)

Crosbie	US 2002/0083343 A1	Jun. 27, 2002 (Jun. 12, 2001)
Gales	US 2003/0084323 A1	May 1, 2003 (Oct. 31, 2001)
Syvanne	US 7,162,737 B2	Jan. 9, 2007 (Oct. 12, 2001)

Mansfield et al, *Towards trapping wily intruders in the large*, Japan Graduate School of Information Sciences, Tohoku University, Sendai, Japan, (1999).

REJECTIONS

Claims 1, 5, 11, 24, and 27 stand rejected under 35 U.S.C. § 102(a) as being anticipated by Mansfield.

Claims 2, 3, 7, 9, 10, and 33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Mansfield and Crosbie.

Claims 4, 6, 12-15, 25, 28-32, and 34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Mansfield and Kim.

Claim 8 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Mansfield, Crosbie, and Kim.

Claim 16 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Mansfield, Kim, and Gales.

EXAMINING TRAFFIC

> When multiple claims subject to the same ground of rejection are argued as a group by appellant, the Board may select a single claim from the group of claims that are argued together to decide the appeal with respect to the group of claims as to the ground of rejection on the basis of the selected claim alone. Notwithstanding any other provision of this paragraph, the failure of appellant to separately argue claims which appellant has grouped together shall constitute a waiver of any argument that the Board must consider the patentability of any grouped claim separately.

37 C.F.R. § 41.37(c)(1)(vii).

Here, the Appellants argue claims 1 and 5 as a group. (App. Br. 10.) The claims of this group are subject to the same ground of rejection. We select claim 1 as the sole claims on which to decide the appeal of the respective group. "With this representation in mind, rather than reiterate the positions of the parties *in toto*, we focus on the issues therebetween." *Ex Parte Zettel*, No. 2007-1361, 2007 WL 3114962, at *2 (BPAI 2007).

> Regarding claim 1, the Examiner makes the following findings.
>
> Mansfield teaches that the collection of statistical information on packets occurs as if the device was disposed on links that are downstream from the links that the provisioned monitor is coupled to (Mansfield, page 6 Section 3.1, traffic monitors traffic entering each site). Mansfield teaches the cited limitation by teaching the traffic monitor disposed on the network link entering each site (Mansfield, Page 6, Figure 4).

(Answer 16.) "Because all packet count information for the link is collected including traffic entering and leaving the data center (see Mansfield, Page 7, Section 3.4, echo and response packets), Mansfield's traffic monitor acts as

if it is disposed on links that are downstream" (*id.*) he further finds. The Appellants ask "[b]y only using packet count, how can Mansfield examine traffic, as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to. Where can Mansfield provide a provisioned monitor by merely keeping a single packet count on each traffic monitor?" (Reply Br. 2.)

> Regarding claim 29, the Examiner also makes the following findings.
>
> Mansfield as modified teaches . . . performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites, Figure 4, sites 1, 2, 3, and 4) . . . .

(Ans. 10-11.) The Appellants argue that "Mansfield does not process statistical information on a per downstream link basis and Kim does not cure that deficiency." (App. Br. 21.)

ISSUE

Therefore, the issue before us is whether the Appellants have shown error in the Examiner's finding that Mansfield teaches a device that examines traffic entering or leaving a data center on links to which the device is coupled as if the device was disposed on links downstream from the coupled links or his finding that the combined teachings of Mansfield and Kim would have suggested performing traffic analysis on a per downstream link basis.

LAW

"[A]nticipation is a question of fact." *In re Hyatt*, 211 F.3d 1367, 1371-72 (Fed. Cir. 2000) (citing *Bischoff v. Wethered*, 76 U.S. (9 Wall.) 812, 814-15 (1869); *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997)). "[A]nticipation of a claim under § 102 can be found . . . if the prior art reference discloses every element of the claim . . . ." *In re King*, 801 F.2d 1324, 1326 (Fed. Cir. 1986) (citing *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.,* 730 F.2d 1452, 1457 (Fed. Cir. 1984)).

"'On appeal to the Board, an applicant can overcome a rejection by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.'" *In re Kahn*, 441 F.3d 977, 985-86 (Fed.Cir. 2006) (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed.Cir. 1998)).

FINDING OF FACT ("FFS")

0. Claim 1 recites in pertinent part the following limitations:

> a device . . . disposed to examine traffic entering or leaving that data center on the coupled physical links and collect statistical information on packets that are sent between the network and the data center over the coupled physical links . . . as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

Similarly, claim 29 recites in pertinent part the following limitations: "performing traffic analysis on the collected statistical information on a per downstream link basis . . . ."

1. Mansfield's "basic concept of signature-based traffic tracing is shown in [its] Fig.4. The traffic monitor collects the relevant packet count information from each link, which connects the sites. The NMS compares the monitored traffic pattern[s], and correlates them." (P. 6.)

2. Figure 4 shows that the traffic monitor is coupled to the links from which it collects information.

ANALYSIS

It is uncontested that Mansfield's traffic monitor collects packet count information from links (FF 1) to which it is coupled (FF 2) and that the reference's NMS compares and correlates the monitored traffic patterns (FF 1). As aforementioned, the Examiner has found that the reference's traffic monitor acts as if it is disposed on links that are downstream. He also has found that the combined teachings of Mansfield and Kim would have suggested performing traffic analysis on a per downstream link basis.

Although the Appellants ask "how Mansfield can examine traffic, as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to" (Reply Br. 2) and "[w]here can Mansfield provide a provisioned monitor by merely keeping a single packet count on each traffic monitor" (*id.*), they have offered no explanation why Mansfield does not examine traffic as if it was device was disposed on downstream links or why the reference's traffic monitor or NMS is not a provisioned monitor. Nor have they offered any explanation why Mansfield does not process statistical information on a per downstream link basis.

CONCLUSION

Based on the aforementioned facts and analysis, we conclude that the Appellants have shown no error in the Examiner's finding that Mansfield teaches a device that examines traffic entering or leaving a data center on links to which the device is coupled as if the device was disposed on links downstream from the coupled links or his finding that the combined teachings of Mansfield and Kim would have suggested performing traffic analysis on a per downstream link basis.

DEDICATED, PRIVATE NETWORK

Regarding claims 2, 3, and 7-10, the Examiner admits that "Mansfield fails to teach the monitoring device being coupled to a control center through a dedicated private network." (Answer 18.) He finds, however, that "Crosbie's SSL connection providing a secure dedicated connection between an IDS system (monitoring device) and the management station (Crosbie, paragraph 0118) meets the limitation of the monitoring device being coupled to a control center through a dedicated private network." (*Id.* at 18-19.) The Appellants argue that "[w]hile this layer is effective in providing secure transmission, it is not a private network nor a dedicated network, but merely another layer in the TCP/IP protocol." (Reply Br. 5.)

ISSUE

Therefore, the issue before us is whether the Appellants have shown error in the Examiner's finding that Crosbie teaches a dedicated, private network coupling a monitoring device to a management station.

LAW

"'A *prima facie* case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art.'" *In re Bell*, 991 F.2d 781, 783 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051 (CCPA 1976)).

FINDING OF FACT

3. Crosbie's "[h]ost-based IDS's [i.e., Intrusion Detection System's] secure communication is built upon the Secure Socket Layer (SSL) protocol for client/server interaction." (¶ [0116].)

> Secure Sockets Layer (SSL) is a widely used standard for securing communications over untrusted networks. SSL prevents unauthorized modification or deletion of data as it flows across the network. In addition, it can detect when an interloper sends messages which purport to be from another machine. It is a general communications protocol and can use a variety of encryption techniques.

(¶ [0117].)

ANALYSIS

As aforementioned, the Examiner admits that Mansfield fails to teach its monitoring device being coupled to a control center through a dedicated private network. We agree with the Appellants that Crosbie's SSL layer "is not a private network nor a dedicated network . . . ." (Reply Br. 5.) Instead, the SSL is a general communications protocol used to secure communications over untrusted networks. (FF 3.)

CONCLUSION

Based on the aforementioned facts and analysis, we conclude that the Appellants have shown error in the Examiner's finding that Crosbie teaches a dedicated, private network coupling a monitoring device to a management station.

GATEWAY

Regarding claims 4 and 6, the Examiner finds that "Kim teaches the use of a gateway to install filters and Mansfield teaches a process to thwart denial of service attacks." (Answer 20.) He also finds that "Mansfield as modified teaches a process to aggregate traffic from the various links and to produce logs and detection heuristics (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8)." (*Id.* 8.) The Appellants argue that "Kim's gateway filters packets and allows packets based SA filtering rules, not network intrusions or DoS attacks." (Reply Br. 6.) They also argue that "[w]hile Mansfield shows counts from probe 1 and probe 2, there is no suggestion that this so called 'aggregation' as the examiner characterizes it, is performed by a process that operates on the claimed gateway." (Appeal Br. 19.)

ISSUE

Therefore, the issue before us is whether the Appellants have shown error in the Examiner's findings that the combined teachings of Mansfield and Kim would have suggested a gateway comprising a process to install filters to thwart DoS attacks or a process to aggregate traffic from the various links.

LAW

"The test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art." *In re Young*, 927 F.2d 588, 591 (Fed. Cir. 1991) (citing *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)). "Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references." *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) (citing *Keller*, 642 F.2d at 425). In determining obviousness, furthermore, a reference "must be read, not in isolation, but for what it fairly teaches in combination with the prior art as a whole." *Id.*

FINDING OF FACT

4. Kim's "integrated security gateway 420 protects the internal network 410 from outsiders. It also prevents unauthorized transmission of data/information stored in the internal network computers to outside." (¶ [0028].) "The integrated security gateway 420 [also] provides packet filtering . . . ." (¶ [0031].)

ANALYSIS

The Examiner's rejection is based on the combined teachings of Mansfield and Kim. For its part, Kim teaches a security gateway for protecting a network. (FF 4.) The Appellants' aforementioned arguments respectively attack Kim and Mansfield individually. Such arguments cannot establish non-obviousness.

CONCLUSION

Based on the aforementioned facts and analysis, we conclude that the Appellants have shown no error in the Examiner's findings that the combined teachings of Mansfield and Kim would have suggested a gateway comprising a process to install filters to thwart DoS attacks or a process to aggregate traffic from the various links.

SEPARATE COUNTER LOGS

Regarding claims 11-16, 24, 25, 27, 28, and 30-34, the Examiner finds that "Mansfield teaches the provisioned monitor maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link) . . . ." (Answer 17.) The Appellants ask "[b]y only using packet count, how can Mansfield examine traffic, as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to. Where can Mansfield provide a provisioned monitor by merely keeping a single packet count on each traffic monitor?" (Reply Br. 2.) The Appellants argue that "each traffic monitor only collects information with one counter." (Reply Br. 4.)

ISSUE

Therefore, the issue before us is whether the Appellants have shown error in the Examiner's finding that Mansfield teaches separate counter logs for each provisioned customer.

ANALYSIS

As aforementioned, Mansfield's traffic monitor collects packet count information from links. (FF 1.) We agree with the Appellants that the traffic monitor does not maintain separate counter logs for different customers.

CONCLUSION

Based on the aforementioned facts and analysis, we conclude that the Appellants have shown error in the Examiner's finding that Mansfield teaches separate counter logs for each provisioned customer.

DECISION

We affirm the rejections of claims 1, 4-6, and 29 but reverse the rejections of claims 2, 3, 7-16, 24, 25, 27, 28, and 30-34.

No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

rwk

Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis CA 95618